EXHIBIT "A"

LAW OFFICE OF STEFANIE L. LAMBERT PLLC
400 RENAISSANCE CENTER
26TH FLOOR
DETROIT, MI 48243

December 28, 2023

The Honorable Jim Jordan
House Judiciary Committee
Subcommittee on the Weaponization of the Federal Government
Committee on Oversight and Accountability
United States House of Representatives
Washington, DC 20515

Dear Ranking Member Jordan:

Thank you for your prompt attention to this matter. Please be advised that my law firm represents Fulton County, Pennsylvania. Fulton County requests Congress to investigate Bill Barr and his role in obstructing a federal investigation related to the November 3, 2020 election and the voting equipment used in the November 3, 2020 election. Additionally, Fulton County requests Congress to investigate the Election Assistance Commission (EAC), Pro V & V (EAC voting system test laboratory) and Dominion Voting Systems, Inc. regarding the certification of voting systems and funds provided by Dominion Voting System, Inc. to Pro V & V for Pro V & V to make a recommendation to the EAC to certify the Dominion brand voting equipment, despite this conflict of interest.

Fulton County's experts have found that a malicious python script was installed on the Fulton County Dominion brand voting equipment and the voting equipment was communicating internationally with Canada. Additionally, it has been determined by experts that the Fulton County Dominion brand voting equipment failed to comply with federal standards set by the Cybersecurity and Infrastructure Security Agency (CIZA), the Defense Information Systems Agency (DISA), and the National Institute of Standards and Technology (NIST).
I am attaching to this letter the September 15, 2023, Speckin Forensics Report for review.

Additionally, Fulton County has obtained testimony from Michael Walker, CEO of Pro V & V. Walker testified that Dominion Voting Systems is providing funds to Pro V & V and Pro V & V then recommends certification to the EAC of the Dominion brand voting equipment. Walker further testified and disclosed that Dominion employees and/or contractors are onsite in the Pro V & V facility and

Dominion employees and/or contractors touch and modify voting equipment at the Pro V & V facility.

Fulton County specifically requests Congress to subpoena William McSwain, a former Assistant United States Attorney (AUSA), working at the direction of Bill Barr, to testify regarding Bill Barr's commands to his subordinates. McSwain has disclosed that Barr prevented and obstructed a federal investigation by the Department of Justice and that AUSAs were instructed to refer election matters to swing state Attorney Generals. In Pennsylvania, Josh Shapiro was serving as State Attorney General and had a conflict of interest because was on the November 3, 2020 ballot and had a personal interest in the outcome of the election. No federal investigation was permitted despite this conflict of interest. Simultaneously, Bill Barr publicly gave the appearance that there were no election law violations or election matters worthy of federal investigation. A timely investigation could have been conducted by the Department of Justice, yet it was prevented by Bill Barr. Fulton County requests a full investigation be conducted by Congress into the actions of Bill Barr and his orders related to election matters while he was serving as Attorney General.

Fulton County has ongoing litigation against Dominion for breach of contract, COUNTY OF FULTON, ET AL., v. DOMINION VOTING SYSTEMS, INC. ET AL., Case No. 1:2022 CV 01639, as well as other litigation, to demand accountability and transparency for the residents of Fulton County. The Attorney General for Pennsylvania, and the Secretary of State of Pennsylvania have failed to address the concerns with the Dominion brand voting systems and have a conflict of interest in doing so as a result of numerous election lawsuits filed against their offices and officials following the November 3, 2020 election.

Fulton County is aware that votes were "flipped" in Northampton County, Pennsylvania during the November 7, 2023 election as a result of an ES & S voting machine "error". Additionally, Fulton County is aware that Williamston Tennessee had an inaccurate vote tally that was discovered by the local official. The EAC was requested to perform an inspection and was unable to determine why the hand counts were different than the Dominion brand machine counts. Ultimately, the EAC was forced to rely on the vendor (Dominion) to disclose that its source code was responsible for the inaccurate vote tally. Allegedly Dominion used a "patch" to correct this problem, but the same version was used in the Maricopa 2022 election where similar problems were observed. The March 31, 2022 United States Election Assistance Commission Report of Investigation Dominion Voting Systems D Suite 5-5 B Williamston County, Tennessee is attached to this letter for review. These are not isolated incidents, in Georgia a candidate received zero votes, despite voting for herself, and the investigation revealed that she not only received one vote, but that she won the election.

For the reasons stated above, Fulton County respectfully requests Congress to act immediately and investigate Bill Barr, the Election Assistance Commission (EAC), Pro V & V (EAC voting system test laboratory) and Dominion Voting Systems, Inc.

Sincerely,

Stefanie Lambert

Speckin Forensics, LLC

120 N. Washington Square, Suite 300
PMB 5068
Lansing, Michigan 48933
517-349-3526 • Fax 954-839-8219

Please Direct Correspondence & Payment Here:
2450 Hollywood Boulevard, Suite 700
Hollywood, Florida 33020
954-763-6134 • Fax 954-839-8219

www.4N6.com

Leonard A. Speckin
Retired Document Analyst

Michael J. Sinke
Retired Latent Print Specialist
Retired Crime Scene Reconstruction
Retired Forensic Document Analyst

Dr. George F. Jackson Ph.D.
Forensic Toxicologist

Erich J. Speckin
Forensic Document Analyst
Ink Dating Specialist

Phillip Matusiak
Computer & Graphics Specialist

Thomas K. Huard Ph.D.
DNA Analyst & Consultant

Marshaun Blake
Arson & Fire Specialist

Anthony A. Milone
Computer & Graphics Specialist
Forensic Document Specialist

Dr. Julie Howenstine
Serologist
DNA Analyst & Consultant
Crime Scene Reconstruction

September 15, 2022

Speckin Forensics was retained to acquire forensic Images of hard drives in Fulton County, Pennsylvania. The images of the drives that are the subject of this report were created on July 13-14, 2022.

A total of six hard drives were tendered for copying and analysis. The hard drives were in the corresponding device and were removed for copying and analysis. The record of the drive and the corresponding machine was recorded. One of the hard drives was not operable at the time of our imaging and therefore was not copied. This can be attempted at a later time with a more time-consuming procedure but has not yet been attempted. The remaining five drives were copied during the time onsite in Pennsylvania. The forensic image of each drive was saved on its own new unused Western Digital 4TB USB hard drive. This allowed for later duplication and examination of the evidence.

Using forensically sound procedures we documented the service tag numbers for all machines and the serial numbers of the corresponding hard drives contained within. Photographs were taken to record this. The drives copied are labeled as follows:

	Service Tag	Computer Name	Serial Number	Machine Model
1	3095PY2	EMSSERVER	59PUPSi1T/ 59PUPSi0T	Dell Precision 3430
3	1FPLNY2	Adjudication01	59OUPRS2T	Dell OptiPlex 3050
4	1FNPHY2	Failed drive	59OUPRRRT	Dell OptiPlex 3050
5	30C4PY2	EMSCLIENT02	59PUPSHNT	Dell Precision 3430
6	30B4PY2	EMSCLIENT01	59PUPSI5T	Dell Precision 3430

The key findings are summarized below:

1. The security measures necessary to harden and secure the machines was not completed. The last update or security patch to the devices shows to be April 10, 2019, and no patches or updates were performed after this date.

2. External USB drives have been inserted on several occasions. We are unaware of any current list of approved external drives that could have been used. Therefore, there is no way to determine if any of the inserted USB drives was from an unauthorized source or if the USB drive further comprised the data or the system.
3. There have been substantial changes to the drives as seen with the inclusion of over 900 .dll files and links created since the date of installation of the Dominion software. This .dll additional pathway is a security breach because of the introduction of an unauthorized script.
4. There have also been no updates to the usernames or passwords as the passwords use default settings like "admin" and "guest". The group policies of the devices remain at default settings which in simple terms allows the username "admin" with password "admin"; complete access to the device.
5. The Adjudication01 workstation has a python script installed after the certification date of the system. This should not be added to the drive after a system has already been certified. This python script can exploit and create any number of vulnerabilities including, external access to the system, data export of the tabulations, or introduction of other metrics not part of or allowed by the certification process.
6. As expected and normal, each of the drives are interconnected in a system to one another. This would be required to provide sharing of data and counts between devices. Because of this networking, unauthorized access any one device, allows unauthorized access to any device connected to the network of devices.
7. An external IP address that is associated with Canada is found on the Adjudication 01. This shows that at least one of the network devices has connected to an external device on an external network. This is the same device that the post certification python script is found.

Procedure:

The hard drives from the computers were removed and connected them to a Forensic workstation. The hard drives were mounted as READ ONLY. Using FTK Imager a bit for bit copy was created using the Expert Witness file format. This is an industry standard format for storing forensic images. During the image creation process a hash value was computed to ensure the integrity of evidence. One of the main uses of hash values is to determine the integrity of data.

The copied data was analyzed using standard computer forensic software generally accepted in the field to search for the elements contained in this report.

Results:

Windows defender was found on the machines which dates to July 2016. No updates have been made since this time. Simply stated this means that viruses or malicious software components created after that date would not be combatted by this protection without the updates.

Further, Dominion published hardening procedures in 2019 that would reduce the chance of the system being compromised and provide additional security measures for the integrity of the system.

Below is a chart that shows external drives that have been connected to the devices examined.

The Dominion voting Systems software was installed on the devices on 04/10/19, 8/16/19 and 8/23/19. This last install date is consistent with the drives Generic, Canyon, and ScanDisk listed below. However, the 2021 drives do not fit this pattern and are unexplained at this point.

Computer Name	Device	Last Connection Date	Connection Time
3095PY2	PNY USB 2.0 Drive	2019-07-31	16:11
3095PY2	Generic USB Flash Drive	2019-08-23	16:54
3095PY2	Canyon USB Drive	2019-08-23	18:07
3095PY2	ScanDisk Cruzer FIT	2019-08-23	18:15
3095PY2	Samsung Flash Drive	2021-04-22	13:49
3095PY2	Kingston Data Traveler	2021-05-03	20:27
1FPLNY2	Samsung Flash Drive	2021-04-30	19:27
1FPLNY2	Kingston Data Traveler	2021-05-05	13:22

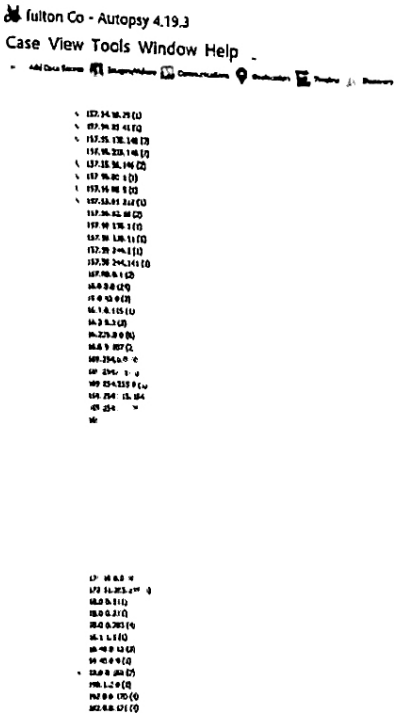
The following chart shows a small sample of .dll activity after the installation date of the voting software.

Name	Deleted	Last Accessed	File Created	Last Written	Entry Modified
UIAutomationTypes.ni.dll	•	08/29/19 08:02:12AM	08/29/19 08:02:12AM	08/29/19 08:02:12AM	10/02/19 04:44:27AM
System.Management.ni.dll		08/29/19 08:02:13AM	08/29/19 08:02:13AM	08/29/19 08:02:13AM	05/18/20 06:50:50AM
UIAutomationProvider.ni.dll	•	08/29/19 08:02:13AM	08/29/19 08:02:13AM	08/29/19 08:02:13AM	10/02/19 04:44:27AM
System.Drawing.ni.dll		08/29/19 08:02:15AM	08/29/19 08:02:15AM	08/29/19 08:02:15AM	10/02/19 04:44:24AM
System.Windows.Forms.ni.dll		08/29/19 08:02:19AM	08/29/19 08:02:19AM	08/29/19 08:02:19AM	10/02/19 04:44:26AM
System.Web.ni.dll		08/29/19 08:02:31AM	08/29/19 08:02:31AM	08/29/19 08:02:32AM	10/17/19 05:55:54AM
System.Messaging.ni.dll		08/29/19 08:02:33AM	08/29/19 08:02:33AM	08/29/19 08:02:33AM	10/17/19 05:55:53AM
System.EnterpriseServices.ni.dll		08/29/19 08:02:34AM	08/29/19 08:02:34AM	08/29/19 08:02:34AM	10/17/19 05:55:52AM

At least six different user and administrator accounts on the devices still have the password "Dvscorp2018!!!". This is the default password for the software at the time of installation. It has never been updated nor was it set to expire as should be the case. This is a glaring issue as this is specifically addressed by the Pennsylvania Secretary of State and referencing NIST.

"All jurisdictions implementing the Democracy Suite 5.5x must ensure that no default passwords are used on any devices and that all passwords are complex and secured. Counties must implement an audit process to review and ensure that no default passwords are used upon equipment install/reinstall and routinely change passwords to avoid any password compromise. The passwords and permissions management must at a minimum comply to the password requirements outlined in NIST 800-63".

The log files for the Adjudication device shows an IP address, 172.102.16.22. This IP address comes back to a location in Quebec, Canada, this is a serious issue to be connected remotely to a Canadian system. We cannot determine when this connection occurred or what data was transmitted, but an external connection was made at some point.



Donald A. Smith

Computer Data Specialist

United States Election Assistance Commission
Report of Investigation

Dominion Voting Systems D-Suite 5.5-B

Williamson County, Tennessee

March 31, 2022

Jonathon Panek
Director, Voting System Testing and Certification

U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

Contents

U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

Introduction

In late 2002, Congress passed the Help America Vote Act of 2002 (HAVA), which created the U.S. Election Assistance Commission (EAC) and vested it with the responsibility of setting voting system standards and providing for the testing and certification of voting systems. This mandate represented the first time the Federal government provided for the voluntary testing, certification, and decertification of voting systems nationwide. In response to this HAVA requirement, the EAC has developed the Federal Voting System Testing and Certification Program.

The EAC's Testing and Certification Program includes several quality monitoring tools that help ensure that voting systems continue to meet the EAC's voting system standards as the systems are manufactured, delivered, and used in Federal elections. These aspects of the program enable the EAC to independently monitor the continued compliance of fielded voting systems. One of these tools is field anomaly reporting.

Election officials may submit notices of voting system anomalies directly to the EAC. An anomaly is defined as an irregular or inconsistent action or response from the voting system, or system component, which resulted in the system or component not functioning as intended or expected. Anomaly reports may indicate a voting system is not in compliance with the Voluntary Voting System Guidelines or the procedural requirements of this EAC Testing and Certification Program.

An informal inquiry is the first step taken when information of this nature is presented to the EAC. The sole purpose of the informal inquiry is to determine whether a formal investigation is warranted. The outcome of an informal inquiry is limited to a decision on referral for investigation. A formal investigation is an official investigation by the EAC to determine whether a voting system warrants decertification. The result of a formal investigation is a Report of Investigation.

Reported Anomaly

On November 3, 2021, the EAC received a report from the Tennessee Secretary of State's (TN SoS) office that they were planning an investigation into an anomaly observed in Williamson County, Tennessee during a municipal election held on October 26, 2021, regarding Dominion D-Suite 5.5-B ImageCast Precinct (ICP) tabulators. Close poll reports from 7 of the 18 ICP tabulators used during the election did not match the number of ballots scanned. Subsequent tabulation on the jurisdiction's ICC central count scanner provided the correct tally. The central count tabulation was confirmed via hand count of the paper ballot records on October 27, 2021.

Discussions with the TN SoS on December 17, 2021, and January 5, 2022, following their investigation, provided additional details to the EAC. The details of the anomaly were

U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

confirmed and reproduced during the state investigation, though the root cause of the anomaly was not determined.

Formal Investigation

Based upon the information obtained from the TN SoS, the EAC initiated a formal investigation into the matter to determine the necessary actions to obtain the root cause and remedy the issue. The investigation was conducted at the Williamson County Elections Commission facility on January 19 through January 22, 2022. This analysis was performed by both EAC accredited Voting System Test Laboratories (VSTL), Pro V&V and SLI Compliance. The EAC, Williamson County staff, TN SoS, and Dominion staff were present during the analysis.

Testing and Analysis

The first step of the VSTL analysis was verification of the system configuration. Hashes of all components involved were collected and compared to the repository of hashes for the EAC certified system. It was discovered that the system was installed with outdated versions of two configuration files when the system was upgraded from D-Suite 5.5 to D-Suite 5.5-B in January of 2021.

Next, a copy of the election definition used on election day was used to make Compact Flash (CF) cards for the ImageCast Precinct (ICP) scanners and ImageCast X (ICX) ballot marking devices. This election definition was imported into the D-Suite 5.5-B system from a definition originally created on the D-Suite 5.5 system.

Ballots were printed from the ICX and tabulated through the ICP scanners. Multiple ICP scanners were used for tabulation including some that originally exhibited the anomaly during the election and some that did not. Following tabulation, close poll reports and audit logs from the ICP scanners were examined. Results showed that the anomaly was recreated on each of the ICP scanners. This process was repeated several times to understand and isolate the details of exactly when the anomaly occurred and circumstances that may have led to the anomaly occurring.

Analysis of audit log information revealed entries that coincided with the manifestation of the anomaly; a security error "QR code signature mismatch" and a warning message "Ballot format or id is unrecognizable" indicating a QR code misread occurred. When these events were logged, the ballot was rejected. Subsequent resetting of the ICP scanners and additional tabulation demonstrated that each instance of the anomaly coincided with the previously mentioned audit log entries, though not every instance of those audit log entries resulted in the anomaly.

Further analysis of the anomaly behavior showed that the scanners correctly tabulated all ballots until the anomaly was triggered. Following the anomaly, ballots successfully scanned

U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

and tabulated by the ICP were not reflected in the close poll reports on the affected ICP scanners.

Additional iterations of testing were performed after updating the configuration files previously mentioned to the proper versions associated with the D-Suite 5.5-B system. The anomaly was recreated using the correct configuration files with the originally programmed election definition.

A final test was performed using an election definition recreated entirely on the D-Suite 5.5-B system with identical parameters to the definition used during the election and for prior testing. The anomaly was not observed during this test, and there were no instances of the security error "QR code signature mismatch" or warning message "Ballot format or id is unrecognizable" in the audit log.

Conclusion of Formal Investigation

The direct cause of the anomaly was inconclusive. Based on the investigation, it's reasonable to conclude that the anomaly is related to the imported D-Suite 5.5 election definition used on the D-Suite 5.5-B system.

On February 11, 2022, Dominion submitted a Root Cause Analysis (RCA) to the EAC. The report indicates that erroneous code is present in the EAC certified D-Suite 5.5-B and D-Suite 5.5-C systems. The RCA report states that when the anomaly occurs, it's due to a misread of the QR code. If the QR code misread affects a certain part of the QR code, the ICP scanner mistakenly interprets a bit in the code that marks the ballot as provisional. Once that misread happens, the provisional flag is not properly reset after that ballot's voting session. The result is that every ballot scanned and tabulated by the machine after that misread is marked as provisional and thus, not included in the tabulator's close poll report totals.

Dominion has submitted Engineering Change Orders (ECO)s for the ICP software in the D-Suite 5.5-B and D-Suite 5.5-C systems: ECO 100826 and ECO 100827. Modified ICP source code was submitted by Dominion that resets the provisional flag following each voting session. The ECO analysis included source code review to confirm the change to both systems and to ensure no other code is changed. A Trusted Build of the modified source code was performed to produce the updated ICP software. This software was then tested for accuracy by processing two thousand ballots printed by an ICX, utilizing the same election definition used in Williamson County, TN on October 26, 2021.

The analysis and testing of the ECOs has demonstrated that the anomaly was successfully fixed. No instance of the anomaly or the associated error or warning messages in the ICP audit logs were observed during the testing. The EAC has approved ECO 100826 and ECO 100827 on March 31, 2022.